OT-CYBER.DE

WOCHENBERICHT

OT-/Cyber-Lagebild Gesamt: alle OT-Branchen

Ausgabe KW 48/2026 · Gesamt: alle OT-Branchen in DACH

Zielgruppe	Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH
Berichtszeitraum	20.11.2026 bis 27.11.2026
Version	1.0
Datum	27.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR, ausschließlich öffentliche Quellen

Dieser Bericht fasst öffentlich zugängliche Meldungen zusammen. Die Einstufung der Relevanz bezieht sich auf Betreiber von Anlagen und Maschinen, KRITIS, Industrie in DACH in Deutschland, Österreich und der Schweiz.

Management Summary

In KW 48 kommen die akuten Risiken für Betreiber in DACH vor allem über Edge-Geräte und Fernwartungswege. Palo Alto bestätigt Angriffe auf PAN-OS-Firewalls, deren Management-Oberfläche aus dem Internet erreichbar ist. CISA hat am 25.11. drei ältere Lücken der Danfoss-Kühlstellen-Manager AK-SM 800A als aktiv ausgenutzt in den KEV-Katalog aufgenommen. Für dieselbe Gerätefamilie gibt es dazu eine neue kritische Lücke ohne Login, für die noch kein Patch vorliegt.

Im Engineering- und Steuerungsumfeld gab es eine dichte Reihe von Advisories. Siemens Industrial Edge hat fünf NGINX-Lücken und noch keinen Fix. WAGO meldet Rechteausweitung bis Root im Web-Based Management, CODESYS Visualization Lücken, über die eine präparierte Runtime den Engineering-PC angreifen kann, und Phoenix Contact eine Kernel-Lücke in mGuard-Gateways (CVSS 9,8). Wer Fernzugang (CC4), Segmentierung (CC2) und risikobasiertes Patchen (CC5) diese Woche abarbeitet, deckt fast alle Meldungen ab.

GESAMTBEWERTUNG

Die Lage ist hoch: Es gibt bestätigte Ausnutzung an Firewalls und Kühlanlagen-Steuerungen, und mehrere kritische ICS-Lücken sind noch ohne Patch. Vorrang haben Management-Oberflächen und Fernwartungszugänge, die aus dem Internet erreichbar sind.

Trends

• Angreifer gehen gezielt auf Edge-Geräte mit offener Management-Oberfläche: Firewalls, VPN-Gateways und fernwartbare Systemmanager sind der erste Schritt in die OT.

• Kälte- und Kühlanlagen-Steuerungen werden zum eigenen Angriffsziel. Alte, längst bekannte Lücken werden aktiv ausgenutzt, weil viele Geräte nie gepatcht wurden.

• Mehrere kritische ICS-Lücken kommen ohne sofort verfügbaren Patch (Siemens Industrial Edge, Danfoss AK-SM8xxA), Schutz bieten bis dahin nur Architektur und Zugangskontrolle.

• Ransomware bei Herstellern wie Osaki Electric legt Lieferketten für Messtechnik lahm, Betreiber spüren das als Lieferausfall und nicht als eigenen Vorfall.

Lageübersicht

ID	Meldung	Relevanz	Quelle
L-01	Palo Alto PAN-OS: Ausnutzung von CVE-2026-46300 über erreichbare Management-Oberflächen bestätigt	KRITISCH	Palo Alto Networks Security Advisory PAN-SA-2026-0015, 25.11.
L-02	Danfoss AK-SM8xxA: Stack-Overflow ohne Login (CVE-2026-129713, CVSS v3.1 9,8), Patch erst mit 5.5.x	HOCH	CISA ICS Advisory ICSA-26-328-03, 24.11.
L-03	Siemens Industrial Edge: fünf NGINX-Lücken, alle Versionen betroffen, noch kein Fix (SSA-935812)	HOCH	Siemens ProductCERT SSA-935812, 20.11.

Exponierte OT-Systeme (Shodan)

Exponierte OT-Systeme (Shodan, Stand 27.11.2026):

Gezählt werden aus dem Internet erreichbare Dienste typischer OT-Protokolle. Die Zahlen sind ein Indikator für Angriffsfläche, kein Nachweis einer Verwundbarkeit. Keine Einzelsysteme genannt. Siemens S7 = Port 102 (alle ISO-TSAP-Dienste, nicht nur echte S7-Steuerungen), OPC UA = Standardport 4840.

Region	Gesamt	Top-Protokolle
Deutschland	136005	DNP3: 31017, OMRON FINS: 24583, ProConOS: 15127, Siemens S7: 7537, OPC UA: 4801
Österreich	4553	HMI/VNC: 998, DNP3: 978, Niagara Fox: 435, Siemens S7: 367, OPC UA: 136
Bayern (München)	1431	OMRON FINS: 788, HMI/VNC: 188, DNP3: 184, Siemens S7: 20, OPC UA: 23
Salzburg	33	HMI/VNC: 10, Niagara Fox: 7, BACnet: 5, Siemens S7: 2, OPC UA: 1
Tirol (Innsbruck)	27	DNP3: 8, Niagara Fox: 6, Modbus: 4, Siemens S7: 2, OPC UA: 1

Meldungen im Detail

L-01 Palo Alto PAN-OS: Ausnutzung von CVE-2026-46300 über erreichbare Management-Oberflächen bestätigt

KRITISCH Palo Alto Networks Security Advisory PAN-SA-2026-0015, 25.11.

Was ist neu: Palo Alto bestätigt, dass die Linux-Kernel-Lücke CVE-2026-46300 („Fragnesia“) gegen die Management-Oberfläche von PAN-OS ausgenutzt wird. Das Advisory wurde am 24.11.2026 erstmals veröffentlicht und am 25.11.2026 aktualisiert. Behoben ist die Lücke unter anderem in 10.2.7-h41, 11.1.4-h40, 11.2.4-h25, 12.1.4-h15 und 12.2.4-h3 sowie in allen späteren Versionen.

Bedeutung: PAN-OS-Firewalls stehen oft zwischen Büro-IT und Leittechnik oder dienen als VPN-Gateway für die Fernwartung. Ist die Management-Oberfläche offen, kann ein Angreifer dort einen Brückenkopf an genau der Stelle aufbauen, die die OT abschirmen soll.

Empfehlung: Den Zugriff auf die Management-Oberfläche sofort auf vertrauenswürdige interne IP-Adressen beschränken und auf eine behobene Version aktualisieren (CC2). War die Oberfläche erreichbar, mit Incident Response nach Kompromittierungsspuren suchen (CC1).

Quelle: https://security.paloaltonetworks.com/PAN-SA-2026-0015 ✓ geprüft

L-02 Danfoss AK-SM8xxA: Stack-Overflow ohne Login (CVE-2026-129713, CVSS v3.1 9,8), Patch erst mit 5.5.x

HOCH CISA ICS Advisory ICSA-26-328-03, 24.11.

Was ist neu: CISA meldet einen Stack-based Buffer Overflow in Danfoss AK-SM8xxA in Version 5.4.0 und älter, der ohne Anmeldung ausnutzbar ist (CVSS v3.1 9,8, v4 9,3). Danfoss plant ein Update auf Version 5.5.x. Öffentliche Ausnutzung ist CISA bisher nicht gemeldet.

Bedeutung: Es ist eine andere Lücke als die drei KEV-Einträge, sie betrifft aber dieselbe Gerätefamilie, die gerade angegriffen wird. Bis zum Patch hilft nur die Netzarchitektur.

Empfehlung: Geräte ohne öffentliche IP-Adresse betreiben, Fernzugriff nur über VPN, alle Geräte im Strict Mode und mit starken, eindeutigen Passwörtern (CC2, CC4). Version 5.5.x einplanen, sobald sie erscheint (CC5).

Quelle: https://www.cisa.gov/news-events/ics-advisories/icsa-26-328-03 ✓ geprüft

L-03 Siemens Industrial Edge: fünf NGINX-Lücken, alle Versionen betroffen, noch kein Fix (SSA-935812)

HOCH Siemens ProductCERT SSA-935812, 20.11.

Was ist neu: Siemens meldet die Lücken CVE-2026-113425, CVE-2026-121810, CVE-2026-123007, CVE-2026-123633 und CVE-2026-123634 in Industrial Edge Cloud Device, Device Kit (arm64, x86-64), Own Device und Virtual Device. Die Bewertung liegt bei CVSS v3.1 8,1 bzw. v4.0 9,2, ausnutzbar über das Netz ohne Anmeldung, aber mit hoher Komplexität. Einen Fix gibt es noch nicht.

Bedeutung: Industrial Edge sitzt direkt an Steuerungen und sammelt Prozessdaten, oft mit Verbindungen in IT und Cloud. Ein kompromittiertes Edge-Gerät wäre ein Sprungbrett in die Zelle.

Empfehlung: Edge-Geräte in eine eigene Zone legen und nur benötigte Verbindungen erlauben (CC2). Die Siemens-Mitigations über WAF oder Reverse Proxy umsetzen: HTTP/2 und HTTP/3/QUIC aus, keine SSI- und Mirror-Direktiven (CC5).

Quelle: https://cert-portal.siemens.com/productcert/html/ssa-935812.html ✓ geprüft

Empfehlungen

Nr.	Maßnahme	Bezug	Priorität	Zeitraum
M-01	Alle aus dem Internet erreichbaren Management-Oberflächen und Fernwartungszugänge (PAN-OS, mGuard, Danfoss AK-SM) schließen oder hinter VPN mit MFA legen [CC4 Secure Remote Access]	L-01	HOCH	sofort
M-02	Siemens Industrial Edge und WAGO-Steuerungen in eigene Zonen mit eng gefassten Kommunikationsregeln legen [CC2 Defensible Architecture]	L-03	MITTEL	0 bis 3 Monate

Fragen für das nächste Jour fixe

1. Ist bei irgendeiner unserer Firewalls oder VPN-Gateways die Management-Oberfläche aus dem Internet erreichbar, und wer hat das zuletzt geprüft?

2. Welche Kälte-, Edge- und Gateway-Geräte (Danfoss, Siemens Industrial Edge, mGuard, WAGO) stehen in unserem Asset-Inventar, mit welchem Firmwarestand?

3. Über welche Wege greifen externe Dienstleister heute auf unsere Anlagen zu, und läuft jeder davon über VPN mit MFA und Protokollierung?

4. Wenn ein Gateway kompromittiert ist: Haben wir einen geübten Ablauf, um es zu isolieren, ohne den Prozess zu stoppen?

5. Welche Lieferanten für Zähler, Steuerungen und Ersatzteile sind kritisch, und wie lieferfähig bleiben sie nach einem Cyberangriff?

Maßnahmen dieser Woche

1. PAN-OS-Firewalls auf behobene Versionen bringen und die Management-Oberfläche auf interne Admin-Netze beschränken. War sie offen, Logs auf Auffälligkeiten prüfen.

2. Alle Danfoss AK-SM-Geräte erfassen, öffentliche Erreichbarkeit abschalten, Strict Mode aktivieren und Standard-Passwörter ersetzen.

3. mGuard-Firmware auf 10.7.1 aktualisieren oder bis dahin den Management-Zugriff per Firewall-Regel sperren.

4. Siemens Industrial Edge isolieren und die Mitigations zu HTTP/2, HTTP/3/QUIC und SSI umsetzen.

5. WAGO-WBM-Konten von Dienstleistern prüfen und den Rollout von Firmware 4.10.0 planen.

6. CODESYS Visualization auf Engineering-PCs und Service-Laptops auf 4.11.0.0 aktualisieren.

HINWEIS ZUR QUELLENLAGE

Alle sieben Meldungen sind gegen die Primärquellen geprüft (Hersteller, CISA, CERT@VDE). VDE-2026-159 erschien am 18.11. und liegt damit knapp vor dem Berichtszeitraum. Außerhalb des Zeitraums und deshalb nicht als Meldung aufgenommen sind der BSI-Lagebericht (19.11., Lage „angespannt bis kritisch“, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/261119_Lagebericht.html), der gezielte Angriff auf die Stadtwerke-Tochter Wittenberg-Net mit rund 8.000 betroffenen Kunden (Volksstimme, 19.11., https://www.volksstimme.de/panorama/nach-it-angriff-in-wittenberg-versorgung-wiederhergestellt-4358944) und die Ransomware bei Osaki Electric (18.11., https://www.osaki.co.jp/ja/notice/20261118.html). Nicht bestätigt und deshalb nicht aufgenommen: ein möglicher Cyberangriff auf SAP (Pressebericht vom 27.11., ohne Primärquelle). Die Danfoss-Advisory zu CVE-2026-127057 war nur über eine Sekundärquelle erreichbar. Für Österreich (NISG 2026) und die Schweiz habe ich im Zeitraum keine belastbare neue Primärmeldung gefunden. Alle Quellenlinks wurden am 27.11.2026 automatisch aufgerufen und inhaltlich geprüft. 4 Meldung(en) ohne überprüfbare Originalquelle oder ohne wörtlichen Beleg wurden nicht aufgenommen.